American Journal of Operations Management and Information Systems
2024, Vol. 9, No. 1, pp. 17-24
https://doi.org/10.11648/j.ajomis.20240901.12

Research Article

The Use of AI to Analyze Social Media Attacks for Predictive Analytics

Temitope Samson Adekunle[1], Morolake Oladayo Lawrence[2], Oluwaseyi Omotayo Alabi[3, *], Godwin Nse Ebong[4], Grace Oluwamayowa Ajiboye[5], Temitope Abiodun Bamisaye[6]

[1]Department of Computer Science, Colorado State University, Fort Collins, USA
[2]Department of Computer Science, Baze University, Abuja, Nigeria
[3]Department of Mechanical Engineering, Lead City University, Ibadan, Nigeria
[4]Department of Data Science, University of Salford, Salford, UK
[5]Department of Computer Science, Precious Cornerstone University, Ibadan, Nigeria
[6]Department of Computer Science, National Open University of Nigeria, Abuja, Nigeria

Abstract

Social engineering, on the other hand, presents weaknesses that are difficult to directly quantify in penetration testing. The majority of expert social engineers utilize phishing and adware tactics to convince victims to provide information voluntarily. Social Engineering (SE) in social media has a similar structural layout to regular postings but has a malevolent intrinsic purpose. Recurrent Neural Network-Long Short-Term Memory (RNN-LSTM) was used to train a novel SE model to recognize covert SE threats in communications on social networks. The dataset includes a variety of posts, including text, images, and videos. It was compiled over a period of several months and was carefully curated to ensure that it is representative of the types of content that is typically posted on social media. First, by using domain heuristics, the social engineering assaults detection (SEAD) pipeline is intended to weed out social posts with malevolent intent. After tokenizing each social media post into sentences, each post is examined using a sentiment analyzer to determine whether it is a training data normal or an abnormality. Subsequently, an RNN-LSTM model is trained to detect five categories of social engineering assaults, some of which may involve information-gathering signals. Comparing the experimental findings to the ground truth labeled by network experts, the SEA model achieved 0.82 classification precision and 0.79 recall.

Keywords

Artificial Neural Network, Cybersecurity, Machine Learning, Random Forest Classifier, Social Engineering Attack

*Corresponding author: alabi.oluwaseyi@lcu.edu.ng (Oluwaseyi Omotayo Alabi)

Received: 26 January 2024; **Accepted:** 5 February 2024; **Published:** 2 April 2024

1. Introduction

Social media platforms have become an important part of daily life for many people, providing a way to connect with others and share information. However, these platforms have also become a tool for spreading misinformation and attacking others. In recent years, there has been a growing interest in using Artificial Intelligence (AI) to analyze social media data for predictive analytics. This can help identify patterns in online attacks and develop strategies for combating them. Facebook now has more users than any other social media platform, and it receives daily billions of visitors. Additionally, during the pandemic, social media usage for online commerce and communication during physical restrictions increased dramatically. The increased usage of social media encourages hackers to utilize security flaws to steal user information [1]. Social media is people-focused, therefore "hacking" the system entails applying social engineering to take advantage of human aspects. One common technique is to pose as peers or bots in chat boxes to get private data [2]. Additionally, any hacker with sufficient skills can communicate with anyone on the planet without the website administrator's consent. For instance, hackers may send spam communications to users while pretending to be banks in order to obtain their passwords or bank accounts. Additionally, hackers can now simply track the activity of real users on social media networks by making straightforward Application Programming Interface API requests. Reconnaissance is a common first step in SE assaults. Before initiating vicious attacks that sound plausible to the victims, the attacker spends a lot of time researching user behaviors, such as their preferred products and routines [3, 4]

Social engineering attacks that target users' moral fallibility are unique because they exploit specific behavioral vulnerabilities in their targets. For example, users who are nervous about succeeding, afraid of taking control, or afraid of failure may be more likely to act rashly and fall victim to these attacks. By understanding these vulnerabilities, it is possible to develop better defenses against social engineering attacks. According to Symantec Security Response, just 4 % of cyber-attacks are brought on by technical flaws and software exploitation methods [5]. Although our findings show that some measures are being taken to protect social media data, the vast majority of the analyzed posts indicated a need for further improvement in data security. This includes the security of both the social media platforms themselves, as well as the applications and devices used to access them. Without these additional measures, users' data remains vulnerable to a variety of threats, including unauthorized access, data breaches, and malware. Ultimately, the current state of social media security leaves much to be desired. No matter the machine type or operating system, network security only stops a small number of threats [6].

HBGary disregarded the Content Management System CMS flaw that causes unauthorized shell access because of incorrect Secure Shell SSH configurations, despite the fact that the security is otherwise quite conventional and simple. The issue is caused by carelessness, a common human error brought on by exhaustion or inexperience [7]. This integration has been used to develop features such as traffic filtering and intrusion detection, which can help to improve the security of social media data. SDN allows for centralized control of a network, while Cisco DNA uses automation and analytics to optimize network performance. Together, these technologies can help to ensure that social media data is protected from unauthorized access and malicious attacks [8, 9]. To our knowledge, no study has yet been done that employs ML to categorize SE threats because of these entities' subjectivity. The types of data needed for SE make acquiring datasets more challenging due to security concerns. Instead of a packet datagram unit, social media posts in our situation are primarily texts written in many languages [10, 11]. Because human characteristics and behavior are continually changing on social media, data collection must be ongoing (rather than done in stages) [12, 13]. Natural Language Processing (NLP) is also necessary for analyzing social media data, since it can process language related to human factors such as fear, anxiety, and other emotions. NLP is able to analyze and interpret unstructured text data in order to extract relevant information and make predictions about user behavior. This is crucial for detecting and preventing social engineering attacks.

In computer networking, artificial neural networks are frequently used for threat detection [14]. Staudemeyer [15], suggests enhancing the classification accuracy of network threats by utilizing network traffic techniques and making the entire process of known harmful activity for detecting assaults. They build a (neural) network with two cells each in each of the four memory blocks. The experimental results of the authors showed that the proposed Long Short-Term Memory (LSTM) model outperformed existing methods because it can track and correlate the continuous communication records over time. Similarly, in our study, we can train LSTM on the phrases in social media posts by treating the sequence of individual words as a time-step sequence. This allows LSTM to learn the underlying patterns in the data and make predictions about the sentiment of the posts.

Meanwhile, an RNN for intrusion detection was created by Krishnan and Raajan [16]. While the use of machine learning in routing technologies like SDN and Cisco DNA can provide significant benefits, there are simpler approaches that can be used to gather threat intelligence. One such approach is to use the Simple Network Management Protocol (SNMP) to monitor network activity and identify potential threats. Another approach is to use a random forest classifier, a type of machine learning algorithm that can identify patterns in large datasets. These simpler approaches may be less complex than integrating machine learning into routing technologies, but

they can still provide valuable insights into potential threats. Despite working with big datasets, the suggested RNN classifies comparable threats more precisely and trains more quickly. Similarly, [17] using the Network Security Laboratory Knowledge Discovery in Databases NSL-KDD dataset, another RNN-LSTM for Intrusion Detection System IDS was trained and its accuracy was compared to that of Subversion SVN, Artificial Neural Network ANN, [18]. It was later shown that this improvement gain is feasible because LSTM overcomes the vanishing gradient drop and fixes the long-term dependency problem when training network data [19, 20]. To describe the spatial and temporal cues of network threats, the upgraded leNet-5 and LSTM neural network structures were directly merged. Deep learning for threat intelligence has long been a source of inspiration for cybersecurity researchers, but these models cannot identify social engineering assaults without network parameters. Instead, semantic sentences, a network and NLP domain hybrid, profiles Search Engine Advertising SEA disguising as social media posts.

In this study, we detect specific SE attack modifications in social media postings, we train an RNN-LSTM model. The datasets provided by the Social Computing Data Repository, SNAP, and Network Repository are all based on older services, and the speed of tweets makes it difficult to obtain enough data to provide meaningful context. Therefore, we decided to crawl Facebook for social media comments instead. Once we had collected a sufficient amount of data, we developed a pipeline for data pre-processing that was specifically designed for the detection of social engineering attacks (SEAD). This pipeline allowed us to clean and prepare the data for analysis, which was essential for the development of ML model [21, 22]. To identify posts that suggest a malicious intent to gather information, the SEADS model uses a variety of variables, including keyword matching, provenance filtering, and pattern recognition. These variables are used to model the language patterns of the posts and assign each one a sentiment score. The model then classifies the posts as SE attacks based on these scores. By analyzing the spatial-spectral language patterns of the posts, the model is able to detect and flag malicious content more accurately. Traditionally, the focus in social media analysis has been to identify and mitigate threats like cyberbullying, hate speech, or malicious content using ML techniques. However, the novel aspect lies in the implementation of deep learning methodologies for attack classifications on social media platforms. This innovative approach involves leveraging the multi-layered neural networks' capabilities to discern more intricate patterns within textual, visual, and contextual data, allowing for a more nuanced and accurate classification of various types of attacks.

2. Method

In Figure 1, we provide a visual representation of how our SEAD tool is used to detect potentially malicious posts on social media. The process starts with crawling data from Facebook and collecting a large dataset of social media posts. Then, the data is pre-processed using natural language processing (NLP) and data cleaning techniques. Next, the data is labeled using machine learning algorithms, and a classification model is trained on the labeled data. Finally, the trained model is used to detect malicious social media posts in real-time. As can be seen in the figure, the tool uses a combination of NLP and ML techniques to identify posts that may be intended to deceive or manipulate users. In our definition of malevolent, pretexting, accusatory, and imperative behavior are included. First, Spyder is used to trawl demographic information from individual Facebook accounts and social media postings from the open posts of random individuals. Then, a recognizer for entities is developed to separate the perpetrator, target victim, and assault target the three primary entities from text-based posts. To categorize texts into predetermined categories such as people, places, organizations, everyday items (digital), device kinds, and actions, entity recognition uses the Natural Language Toolkit NLTK and SpaCy framework. For instance, "It was posted on Facebook that "Public Bank Customer Care has noticed a change in the password for your user account Seyi." The tuplet's three essential parts formed by the social media posts are "subject: customer service, victim: Seyi, and target: passwords."

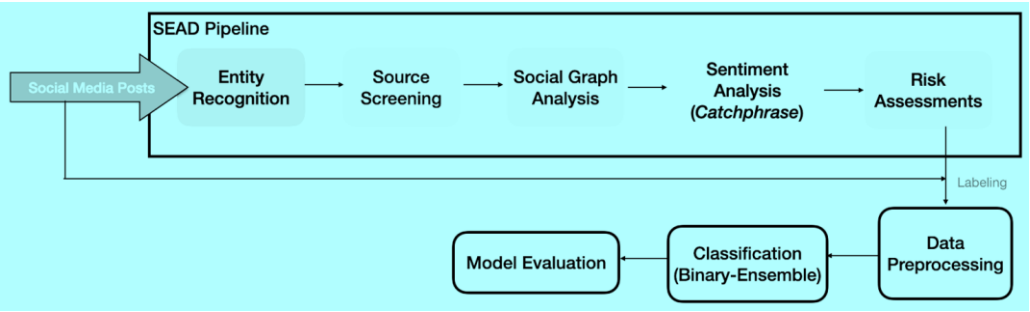

Figure 1. *The Pipeline for Social Media Engineering Attack Classifications (Aun et al., 2023).*

2.1. Data Input Analysis

SEAD functions on the presumption of guilt unless innocence is established. Utilizing subject screening and filtering methods like Tesseract, SEAD is geared up to immediately ban SEA threats. The input data analysis is comparable to stateful firewalls' blocking of signals. A building blacklist database's user accounts and known IP addresses of criminal people and botnets are compared to the previously recognized subjects and perpetrators. Input data analysis, in contrast to firewalls, searches for application layer potential dangers to spot hacked accounts with malicious intent. In addition to examining network headers like IP addresses, our model also considers the directionality of conversations, as illustrated in Figure 2. This means that if a malicious source is replying to a legitimate user who started the conversation, it is less likely to be flagged as suspicious. This is because the original message from the legitimate user is already part of the conversation and is therefore less likely to be malicious. This approach improves the accuracy of the model and helps to reduce false positives.

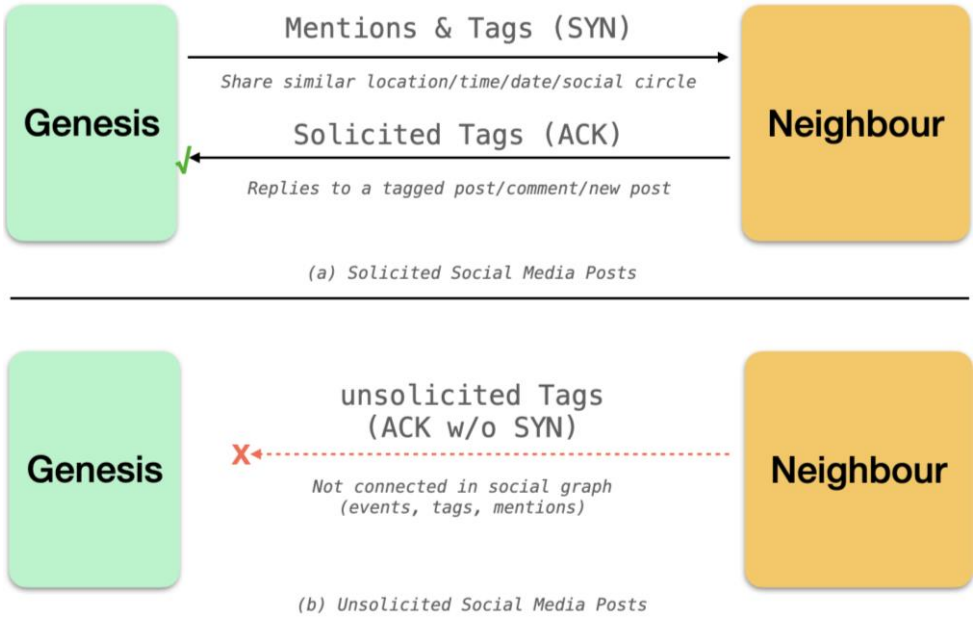

Figure 2. *Depending on the interaction state, calculating the maliciousness index of social media posts. A legitimate post in (a) must be asking for previous encounters. If there haven't been any past interactions between the circles, a post with similar semantics in (b) gets red-flagged (Aun et al., 2023).*

2.2. Detection Method Based

Measurement methods frequently include sentiment analysis. To construct a sentiment analyzer that can identify SE assaults on social media posts, we use Google Auto ML. Because post models now in use express positive sentiment using positive adjectives and negative sentiment using negative adjectives, we need to develop a special sentiment analysis model [9, 23]. For instance, the present sentiment model will not detect the phrase "borrowing your account for emergencies" as a SE assault, despite the fact that it should. SEAD trains for a set of keywords that have malicious intentions using a bespoke Name-based entity recognition (NER). There are two steps at the core of NER. The NER initially looks for a word(s) that make up an entity. It's usual practice to tag entities with an inside-outside-beginning to denote their beginning and end [24, 25]. The identified entities are then classified by NER into significant categories, such as person, organization, location, and in our instance, activities that suggest hostile intents. Two experts assign a morphology-based label of "0" or "1" to dataset of instant each post, Label "0" denotes a benign social media message, such as "ideal conditions for hanging out," while label "1" denotes a potential SE assault, such as "steal your account."

2.3. Data Labeling and Risk Analysis

SEAD determines SEA's "integrity" across all social media post by averaging the threat factor across three detection components when doing risk analysis [26, 27]. On the basis of heuristics, each individual component is initially graded on a scale from 0 to 1. Each of the three factors is given equal weight. When a social media post's integrity has been compromised, such as when it was uploaded by an account or contains references to other accounts with verified identities,

it is marked as true (1) during source screening a bad reputation, or vice versa. In the meantime, the post is marked as true (1) in the social graph to denote an indirect post, which includes postings that do not respond to prior interactions or mentions from unrelated personal and professional accounts. Last but not least, the sentiment analysis determines the sentiment score for each article based on professional keywords (One for positive and zero for negative). SEAD assesses whether a post has SEA elements based on these combined scores; a score of 0.5 is deemed safe (0) while a value of >0.5 is deemed hostile (1).

3. Results and Discussion

3.1. Datasets and Attack Classes

We constructed a five-class machine learning model to categorize variations of SEA threats found in Facebook postings because the linguistic character of SEA in social posts is predictable. Since SEA threats center on the SEAD components, Table 1 provides examples of risk analysis of social media posts using those data. For the model training, we choose 5,000 Facebook posts with risk analysis scores greater than 0.5. Five categories—pretexting, phishing, scareware, clickbaits, and quid pro quo are assigned to the dataset by two annotators. To avoid data imbalance, each assault class has an equal 1000 instances. The reliability of the data sets is examined, and any label inconsistencies are debated and resolved by the experts in accordance with their consensus. The classes are described as follows:

1. *Pretexting* - Posts on social media in which the author adopts the personas of coworkers, law law enforcement, banking, and tax officials, or other anyone in a position to know. The pretexter asks questions that are ostensibly required to confirm the victim's identification. To get the essential personal information, they develop wordlists for password guessing and cracking.
2. *Phishing* - Email and SMS communications delivered by attackers pretending to be from a reliable and trusted source are known as phishing scams. These tactics take use of the victim's interest or terror to cause an illogical response to allegations of stolen credit cards, leaked images, and other sentimental material. The majority of the time, the victims are tricked into opening infected attachments or clicking on links to nefarious websites.
3. *Scareware* - In order to trick people into believing that their system or user accounts have been compromised, scareware masquerades as pop-up notifications while they are browsing. Users are duped, and as a defense, they install suggested anti-threat tools which are frequently risks themselves. As opposed to phishing, scareware is more relevant to actual user activities and contexts, which deceives people and lets down their guard.
4. *Click baits* - The victim is baited into falling into the social engineering trap by being shown something enticing. For instance, skillfully worded email subject lines, free music downloads, or gifts with surveys Rewards are worthwhile and deserve a few clicks. While some social engineering attempts may be obvious, such as free mp3s that contain malware or free wallpapers that contain cryptocurrency mining software, the incentives for these attacks often go beyond what is immediately apparent. Attackers may be looking to steal personal information, gain access to sensitive systems, or even manipulate public opinion. It is important to be aware of the wide range of potential incentives for social engineering attacks, as this can help to identify suspicious activity and prevent harm. When individuals encounter deals that seem too good to be real, clickbait frequently succeeds against the weaker defense.
5. *Quid Pro Quo* - a social engineering technique in which the attacker tries to exchange information for a service. These attacks prey on human weaknesses like curiosity and worry and are directed at less tech-savvy individuals. For instance, when faced with technical problems, end customers are more inclined to comply with IT assistance requests and freely divulge credentials for speedy solutions. Working from home has become more common in recent years, but few security landscapes have been thoroughly researched to identify possible vulnerabilities. An effort to use social engineering to trade services for information. These assaults take the use of feelings like curiosity and worry to prey on less tech-savvy individuals. Although remote login is more frequently used these days for working from home, few security landscapes have been thoroughly investigated to identify potential threats.

Table 1. *Risk analysis of social media posts (Test: Train).*

SEA Types	Training		Testing	
	Instance Count	Word Count	Instance Count	Word Count
Pretexting	810	10102	205	2356
Phishing	810	11978	205	2056
Scareware	810	8013	205	1985

SEA Types	Training		Testing	
	Instance Count	Word Count	Instance Count	Word Count
Clickbaits	810	10010	205	2435
Quid Pro Quo	810	9284	205	2006

3.2. Performance Assessment

Since there is no standard benchmark to evaluate how well our model generalizes to new data, we tested its precision and recall against a variety of well-known machine learning algorithms using a synthetic dataset. This dataset was designed to simulate real-world social media data and included features such as text, emojis, and other variables. The results showed that our LSTM model outperformed the other algorithms in terms of both precision and recall. This suggests that the model is capable of generalizing to new data and is robust to noise and variation in the data. Since common datasets like KDD Cup 99 and NSL-KDD don't have the necessary feature set, we employ 1,000 unseen samples that have been marked by professionals as the actual ground truth for model testing. Table 2 demonstrates that the proposed DNN-LSTM outperforms the other models on all measures, scoring 0.85 for precision and 0.80 for recall. The recall rate is generally a little lower, which is typical for multi-class categorization of lengthy, unstructured texts. Longer sentences are difficult for traditional ML predictions because they are typically based on term frequency and a bag of terms. Surprisingly, despite being lighter and faster to train, typical ML-like KNN, DT, and RF hardly outperform neural networks in terms of performance. The decision tree (DT) algorithm is known to be effective at classifying text data when the data is simple and straightforward. The k-nearest neighbor (KNN) algorithm is a clustering technique that can be used for classification without the need for large training datasets. Random forest (RF) is an ensemble technique that combines multiple decision trees to improve accuracy and generalization. In this case, we found that RF outperformed both DT and KNN, likely due to the complex and varied nature of social media data. The disparity between PCA and DBN, on the other hand, is more severe since these algorithms classify words in a sentence as independent entities, losing certain spatial signals to the phrase's linguistic features. MLP, which is slightly less accurate than LSTM, also utilizes forward/backward propagation on a neural network to learn the meaning with the best NN settings and hyperparameters, we contrast an optimized LSTM with an MLP. We ramify that sentence structure, including word choice and the relative order of occurrences, may include useful temporal information. The inclusion of the memory cell in the LSTM architecture allows for the error gradient to be propagated at each level of the learning process, which promotes desired behavior. While we cannot fully explain the inner workings of the neural network model, it is likely that the ability to train the model on entire sentences rather than individual words gives it an advantage over traditional machine learning algorithms. However, it is important to note that neural networks are often considered "black box" models due to the difficulty of interpreting their inner workings When intentions are inferred from words, we conclude using LSTM that it is difficult to create a nearly perfect model. We must first take into account the linguistic literacy gap when comparing intrinsic SEA intentions stated in words. Additionally, circumstances like timing, subjects, the criminal past of the author, the post's subject, and the political and cultural context of the participants are missing when SEA on social media is detected. In other words, certain social engineering attacks don't have verbal expressions and aren't ever represented by any linguistic semantics.

Table 2. *A comparison of the SEA's Classification Precision and Recall for a number of well-known Classifiers.*

Algorithm	Precision	Recall
DT(j47)	0.74	0.69
DBN	0.59	0.50
KNN	0.72	0.65
RF	0.80	0.74
PCA	0.53	0.44
DNN(LSTM)	0.85	0.79

4. Conclusion

Social media posts are becoming a target for social engineering assaults (SEA). In order to trick victims into clicking on dangerous links and unwittingly disclosing critical information, they prey on their fears and insecurities. In order to lessen suspicion, attackers have become closer and more personal in their social media posts recently, making them sound like most other posts yet carrying an inherent motivation. Based on the SEAD pipeline is made to automatically categorize a social media post as harmful or legitimate based on source screening, social graph analysis, and sentiment

analysis. We discover that the majority of SEA may be halted by closely examining postings made by dubious accounts at the source level. The LSTM model outperformed traditional machine learning algorithms, likely due to its ability to process whole sentences rather than individual words. This research is important for improving the safety of social media platforms and helping users to protect themselves from potential harm. Further research is needed to explore how these algorithms can be applied to real-world data and to understand the specific factors that lead to successful predictions.

Abbreviations

SE: Social Engineering
SEAD: Social Engineering Assaults Detection
AI: Artificial Intelligence
ML: Machine Learning
RNN: Recurrent Neural Network
LSTM: Long Short-Term Memory
API: Application Programming Interface
NLP: Natural Language Processing
SDN: Software-Defined Networking
DNA: Digital Network Architecture
CMS: Content Management System
SNMP: Simple Network Management Protocol
NSL: Network Security Laboratory
KDD: Knowledge Discovery in Databases
ANN: Artificial Neural Network ANN

Conflicts of Interest

The authors declare no conflicts of interests.

References

[1] Aldawood, H., & Skinner, G. (2019). *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review*. *December*, 62–68.(Aldawood & Skinner, 2019) https://doi.org/10.1109/tale.2018.8615293

[2] Tanwar, S., Paul, T., Singh, K., Joshi, M., & Rana, A. (2020). Classification and Imapct of Cyber Threats in India: A review. *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 129–135. https://doi.org/10.1109/ICRITO48877.2020.9198024

[3] Ajagbe, S. A., & Adigun, M. O. (2023). Deep learning techniques for detection and prediction of pandemic diseases: a systematic literature review. In *Multimedia Tools and Applications* (Issue 0123456789). Springer US. https://doi.org/10.1007/s11042-023-15805-z

[4] Dasgupta, S., Piplai, A., Kotal, A., & Joshi, A. (2020). A Comparative Study of Deep Learning based Named Entity Recognition Algorithms for Cybersecurity. *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*, 2596–2604. https://doi.org/10.1109/BigData50022.2020.9378482

[5] Lorenzen, C., Agrawal, R., & King, J. (2019). Determining Viability of Deep Learning on Cybersecurity Log Analytics. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, *April*, 4806–4811. https://doi.org/10.1109/BigData.2018.8622165

[6] Gümüşbaş, D., Yıldırım, T., Genovese, A., & Scotti, F. (2021). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal*, *15*(2), 1717–1731. https://doi.org/10.1109/JSYST.2020.2992966

[7] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, *8*, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

[8] Temitope S. Adekunle; Morolake O. Lawrence; Oluwaseyi O. Alabi; Adenrele A. Afolorunso; Godwin N. Ebong; Matthew A. Oladipupo. (2023). Deep Learning for Plant Disease Detection. *Computer Science and Information Technologies*, *5*(1), 49–56. https://doi.org/10.11591/csit.v5i1.pp49-56

[9] Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

[10] Bakhshi, T. (2018). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. *Proceedings - 2017 13th International Conference on Emerging Technologies, ICET2017*, *2018-Janua*, 1–6. https://doi.org/10.1109/ICET.2017.8281653

[11] Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222

[12] Dan, A., & Gupta, S. (2019). Social engineering attack detection and data protection model (SEADDPM). In *Advances in Intelligent Systems and Computing* (Vol. 811, Issue January). Springer Singapore. https://doi.org/10.1007/978-981-13-1544-2_2

[13] de Coning, A., & Mouton, F. (2020). Water distribution network leak detection management. *European Conference on Information Warfare and Security, ECCWS*, *2020-June*(June), 89–97. https://doi.org/10.34190/EWS.20.088

[14] Shafiei, D., Mostafavi, S. A., & Mehrabadi, S. J. (2023). Geometrical optimization of city gate station's water bath indirect heater to minimization of fuel consumption. *Journal of Thermal Engineering*, *9*(4), 841–860. https://doi.org/10.18186/thermal.1325287

[15] Giboney, J. S., Schuetzler, R. M., & Grimes, G. M. (2021). Developing a measure of adversarial thinking in social engineering scenarios. *Proceedings of the 16th Pre-ICIS Workshop on Information Security and Privacy*, 1–15.

[16] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information (Switzerland)*, *10*(4). https://doi.org/10.3390/info10040122

[17] Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8872923

[18] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*(c), 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[19] Le, T. T. H., Kim, J., & Kim, H. (2017). An Effective Intrusion Detection Classifier Using Long Short-Term Memory with Gradient Descent Optimization. *2017 International Conference on Platform Technology and Service, PlatCon 2017 - Proceedings*, *February*. https://doi.org/10.1109/PlatCon.2017.7883684

[20] Zhang, T. tian, Elsakka, M., Huang, W., Wang, Z. guo, Ingham, D. B., Ma, L., & Pourkashanian, M. (2019). Winglet design for vertical axis wind turbines based on a design of experiment and CFD approach. *Energy Conversion and Management*, *195*(February), 712–726. https://doi.org/10.1016/j.enconman.2019.05.055

[21] Akande, T. O., Alabi, O. O., & Ajagbe, S. A. (2024). A Deep Learning-Based CAE Approach For Simulating 3D Vehicle Wheels Under Real-World Conditions. *Journal of Artificial Intelligence and Applications*, 1–16. https://doi.org/10.47852/bonview42021882

[22] Aun, Y., Gan, M. L., Wahab, N. H. B. A., & Hock Guan, G. (2023). Social Engineering Attack Classifications on Social Media Using Deep Learning. *Computers, Materials and Continua*, *74*(3), 4917–4931. https://doi.org/10.32604/cmc.2023.032373

[23] Abdulmajeed Aljuhani, & Abdulaziz Alhubaishy. (2020). 3rd ICCAIS 2020 : International Conference on Computer Applications & Information Security : 19-21 March, 2020, Riyadh, Kingdom of Saudi Arabia. *Incorporating a Decision Support Approach within the Agile Mobile Application Development Process*, 23–26.

[24] Luo, Z., Cai, W., Li, Y., & Peng, D. (2011). The correlation between social tie and reciprocity in social media. *Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology, EMEIT 2011*, *8*, 3909–3911. https://doi.org/10.1109/EMEIT.2011.6023913

[25] Alexan, W., Mamdouh, E., Elbeltagy, M., Ashraf, A., Moustafa, M., & Al-Qurashi, H. (2022). Social Engineering and Technical Security Fusion. *International Telecommunications Conference, ITC-Egypt 2022 - Proceedings*, *August*. https://doi.org/10.1109/ITC-Egypt55520.2022.9855761

[26] Ojo, O. S., Oyediran, M. O., Bamgbade, B. J., Adeniyi, A. E., Ebong, G. N., & Ajagbe, S. A. (2023). Development of an Improved Convolutional Neural Network for an Automated Face Based University Attendance System. *ParadigmPlus*, *4*(1), 18–28. https://doi.org/10.55969/paradigmplus.v4n1a2

[27] Ajagbe, S. A., Adegun, A. A., Olanrewaju, A. B., Oladosu, J. B., & Adigun, M. O. (2023). Performance investigation of two-stage detection techniques using traffic light detection dataset. *IAES International Journal of Artificial Intelligence*, *12*(4), 1909–1919. https://doi.org/10.11591/ijai.v12.i4.pp1909-1919